Office of the Information and
Privacy Commissioner of Alberta

Strategic Business Plan

2015-2018

Office of the Information and Privacy Commissioner

The Information and Privacy Commissioner of Alberta (the Commissioner) is an independent Officer of the Legislature and reports directly to the Legislative Assembly.

Through the Office of the Information and Privacy Commissioner (OIPC), the Commissioner performs the legislative and regulatory responsibilities set out in the following laws:

- the *Freedom of Information and Protection of Privacy Act* (FOIP),
- the *Health Information Act* (HIA), and
- the *Personal Information Protection Act* (PIPA)

The Commissioner is generally responsible for monitoring the administration of these laws (the Acts) to ensure their purposes are achieved.

More specifically, the Commissioner's statutory powers and duties include, but are not limited to:

- Providing independent review and resolution on requests for review of responses to access to information requests and complaints related to the collection, use and disclosure of personal and health information
- Conducting investigations on any matters relating to the application of the Acts
- Conducting inquiries to decide questions of fact and law and issuing binding orders
- Receiving comments from the public concerning the administration of the Acts
- Giving advice and recommendations of general application respecting the rights or obligations of stakeholders under the Acts
- Engaging in or commissioning research into any matter affecting the achievement of the purposes of the Acts
- Commenting on the implications for freedom of information or for protection of personal privacy of proposed legislative schemes and existing or proposed programs
- Commenting on the implications for access to or protection of health information
- Commenting on the privacy and security implications of using or disclosing personal and health information for record linkages or for the purpose of performing data matching

Vision

A society that values and respects access to information and personal privacy.

Mission

The OIPC's work toward supporting its vision includes:

- Advocating for the privacy and access rights of Albertans
- Ensuring public bodies, health custodians and private sector organizations uphold the access and privacy rights contained in the laws of Alberta
- Providing fair, independent and impartial reviews in a timely and efficient manner

Environmental trends and issues

A number of environmental trends and issues shape and influence the work of the OIPC.

One of these trends is the rise of social media and the increasing degree to which **individuals are willing to share information about themselves online** – whether to obtain something tangible (goods and services, shopping discounts), feel connected to others, or to engage with society. Individuals are sharing vast amounts of personal information through blogs, social networks, e-mail, web logs, cell phone GPS signals, call detail records, Internet search indexing, digital photographs, video archives, and through online purchase transactions.

Governments and businesses also use social media to communicate – they blog, tweet, post to YouTube, have Facebook pages, etc. to get their message out and to receive feedback. In addition, information knows no boundaries; it flows across borders and around the globe, with technology as the common denominator that connects everything together.

As a result, businesses and government have the ability to collect an enormous amount of information about citizens. This, coupled with the development of exceptional technologies that allow vast amounts of data to be stored and analyzed in ways never previously contemplated, has led to a phenomenon that has come to be known as **"Big Data."**

Big Data refers to the ability to track and analyze everything from online purchases to the latest Twitter trending topics. It offers massive opportunities for real-time intelligence about responses to products, services and even political decisions. The advantages for businesses are obvious: companies want to listen to what is being said about them and leverage this information for marketing or reputation management purposes. Big Data enhances a business's ability to meet customer expectations, provide better customer service, and improve consumer products. In the world of Big Data, consumer information has value.

The same can be said for health information. In Alberta, efforts have been underway for years to encourage and facilitate the implementation of electronic medical records, to build the **provincial electronic health record** (Netcare) and to connect with systems in other provinces. In many ways, Alberta is leading the country in endeavors such as the adoption of electronic medical records.

The potential benefits of electronic health records for patients and society in general are significant, including the ability to ensure that comprehensive and timely patient information is available to healthcare practitioners and for reducing workplace inefficiencies. A vast electronic repository of health information also holds incredible research potential for improved treatments, quality of care, patient safety and other purposes such as policy development. Patient health information has value.

We are also seeing an increased government focus on **multi-agency citizen-centred service delivery** in all jurisdictions, including Alberta. This global trend seeks to replace the traditional delivery of public services by myriad, disparate government agencies with a network of public, private and non-profit groups that come together to achieve a common mission or program outcome. This new service delivery model recognizes that the social and economic challenges

facing citizens are complex and require interaction between government and community-based providers; it may also hold some promise for reducing government inefficiencies and bureaucracy. The foundation that underpins multi-agency citizen-centred delivery of government services is **information sharing** beyond the sectoral boundaries of private, public, and health, and, in some cases, across provincial and national borders.

At the same time as government is re-evaluating how it delivers programs and services, we increasingly hear commitments to **"accountability," "transparency" and "openness."** These terms are so frequently used as to risk becoming cliché; however, the principles of government accountability and transparency and the public's right to access information held by public institutions are as current and essential as ever. It is access to information that allows citizens to scrutinize government decisions and actions and, as a result, to more fully and effectively participate in the democratic process.

The emphasis on accountability and transparency goes hand in hand with the rise of global **open government and open data** movements.[1] At national, provincial and municipal levels in Canada, governments are committing to initiatives that advance open government and open data agendas. One of the fundamental principles of the open data movement is that information datasets must be available in standard machine-readable formats – to facilitate analysis and manipulation of the data, as well as mash-ups with datasets from multiple sources, including other governments, in other jurisdictions. Another emerging trend is to facilitate open government and open data by developing protocols to ensure that information systems are designed and built with principles of access in mind. These initiatives underscore that information about government decision-making is essential to democracy. Citizens value information about government.

Governments also value information about citizens. This is evidenced by an increased emphasis on **citizen engagement** and government consultation strategies, often employing the use of web tools (government blogging, Tweeting, online forums, etc.). Moreover, the public is increasingly willing to use the Internet and social media to engage with government, and to advocate or lobby for causes.

The prevalence of mobile devices – smart phones, laptops, iPads, USB keys – means that **information is always on the go**, never stationary, and certainly not confined to any one jurisdiction. Geo-location technologies, such as Radio Frequency Identification Devices (RFIDs) and GPS tracking, are specifically designed to monitor the location of things – such as mobile devices – as well as people. All of these devices, and many more, are increasingly connected to the Internet and to each other. One of the most significant emerging trends in technology is said to be the Internet of Things. Some projections suggest that up to 100 billion uniquely identifiable objects will be connected to the Internet by 2020.

Governments, businesses and health custodians alike are looking to technology solutions to maximize efficiencies and reduce costs. **Cloud computing environments**, for example, are increasingly seen as a preferred choice, notwithstanding the possibility that information might be stored on servers in far-flung jurisdictions.

[1] Open government, as used here, is more generally about the proactive and routine release of information to citizens; open data refers to offering government data in a more useful and machine-readable format to enable citizens, the private sector and non-government organizations to leverage it in innovative and value-added ways.

Joining disparate databases together in integrated information systems, as well as the need to uniquely identify someone in the online environment, requires diligent attention to **identity management.** Biometric technologies – facial recognition, fingerprinting, palm vein and iris scanning – are under constant development and are being deployed in new and previously unforeseen ways. Reflecting our interconnectedness and borderless society, provincial, national and international initiatives are underway that are focused on standardization and interoperability of identity management systems.

Implications for access and privacy

The integrated, interconnected, cross-sectoral and often highly technical initiatives described above offer many potential benefits for individuals and society; however, these initiatives also raise a host of access, privacy and data security issues.

For initiatives that involve multiple participating stakeholders, for example, it is imperative to establish **appropriate governance and accountability** structures to ensure that basic responsibilities under access and privacy legislation can be met (e.g. limiting collection, restricting use, responding to access requests, security breaches, etc.).

Cross-sectoral initiatives may also run into **inconsistent legislative requirements**. For example, health custodians, unlike public bodies or private sector businesses, are legally required to submit a Privacy Impact Assessment (PIA) to the OIPC for review and comment before implementing new information systems. Non-profit participants may or may not be subject to access and privacy legislation. Private sector organizations have a duty to report certain privacy breaches to the OIPC, while other participating stakeholders may not have the same obligation. Inconsistent legislative requirements can result in potential risks to personal and health information not being identified or assessed.

Establishing **legislative authority to share information can be complex**, and is made even more so when participants are subject to more than one of the Acts (e.g. a health professional, such as a psychologist or physiotherapist, in independent practice may normally be subject to PIPA but if contracted to the Workers' Compensation Board, he or she may fall under the FOIP Act). When operational staff do not understand the application of the Acts, this creates confusion as to what they can or should do with respect to personal and health information.

Transparency can also be an issue. **Complex, integrated information systems initiatives are often not well understood** by sophisticated users, much less the individuals whose personal or health information may be stored in them. Given this, it may be a challenge for individuals to exercise their rights under access and privacy laws – whether to complain about the collection, use or disclosure of their information, or to request access to it.

Large databases and advanced analytics provide a **temptation to use information for new purposes** other than those for which the information was collected. There are situations in which individuals would likely not object to their information being used for other purposes – for example, the use of health information for research purposes. Studies have shown that most patients are not concerned that their information will be used for research purposes, and would in fact be surprised if this were *not* the case. What they do expect, however, is that health information that is used for research purposes will be subject to strict protocols and safeguards. Alberta's HIA

was designed to facilitate health research within such a system of controls.

Instead, individuals are often more concerned with **secondary use of information for public safety purposes**. Massive amounts of information collected, warehoused, and integrated, are sometimes seen as a silver bullet, guaranteeing a safer society. Often, new initiatives will trade-off privacy rights in the quest for more security. Any such re-purposing of information for public safety, or new collections of information, must be scrutinized closely and demonstrably necessary. The risk is that often only a single initiative is considered at any one time, and the slippery slope trend towards a surveillance society goes unnoticed.

Vast databases of information also present a tempting target for identity thieves and fraudsters. While most **privacy breaches** reported to the OIPC relate to human error and mailing and transmission errors (fax and email), a significant number are the result of database hacks or phishing scams – that is, a targeted attempt by thieves to gain access to personal information for nefarious purposes. Many other breaches are also technology-related in that they involve the loss or theft of computer equipment, and particularly unencrypted mobile devices. Technology-related breaches are particularly egregious in that the number of affected individuals can be enormous.

A particularly disturbing occurrence is unauthorized access by an authorized user of an information system; that is, when a trusted user abuses his or her access privileges to "snoop" on others. While most authorized users of information systems are properly trained and respectful of privacy laws, it remains the case that unauthorized access by authorized users continues to occur and can be very difficult to identify.

Finally, **open government and open data** initiatives, while providing opportunities for citizens to have routine access to information about government decision-making, and reducing the burden on already strained formal access to information processes, can also give rise to privacy risks. Careful thought and planning must go into any decision to publish machine searchable data to ensure privacy is protected. Personal identifiers may be removed, but there are many examples where **seemingly disparate information elements can be combined and linked back to specific individuals**. It can be difficult to determine in advance which seemingly harmless data elements can be combined in such a manner.

Challenges for the OIPC

1. Meeting public and stakeholder expectations for timely resolution of complaints, requests for review

There has been an 11% increase in the number of cases opened by the OIPC since 2011-12 (not including intake cases). The complexity of cases has also increased, as evidenced by more parties, more represented parties, more complex issues (including technology-related cases such as HIA PIAs, solicitor-client privilege), and more cross-sectoral issues. Increasing complexity requires more time to investigate, research and resolve.

An increase in access-related cases is another challenge for the OIPC. Over the last two years, the Office has seen:

- the number of FOIP-related cases opened has increased from 33% of total cases to 43%;
- a 48% increase in the number of requests to review responses to access requests made under FOIP;
- a 125% increase in the number of requests to the Commissioner for time extensions to respond to access requests under FOIP;
- the number of requests to excuse fees increased from 6 in 2011-12 to 33 in 2013-14 (a 450% increase).

The OIPC prioritizes these types of cases to avoid contributing to delays in access. However, as the number of these cases continues to rise, OIPC staff workloads are increasingly made up of high-priority files.

Self-reported breach files are also a priority for the Office, particularly if there is a risk of harm and affected individuals have not been notified. Although the total number of self-reported breach cases under the three Acts has remained relatively constant for the past two years (a 5% increase, from 177 cases to 186), anticipated amendments to the HIA are expected to significantly increase the number of breaches reported to the Office in the future.

The Government of Alberta's review of the FOIP Act also has the potential to significantly impact the OIPC's ability to meet expectations for timely resolution of cases. While the results of the review and any proposed amendments are not known at this time, the OIPC's submission to the review process recommended mandatory breach reporting and notification for public bodies subject to FOIP.

The OIPC's submission also recommended that privacy impact assessments (PIAs) be mandatory for certain kinds of initiatives. The Office's experience under the HIA (which has a mandatory PIA requirement for health custodians) has demonstrated the value of completing PIAs for new initiatives, particularly those that are focused on implementing new technologies or for information sharing initiatives. Should such amendments be made, however, the OIPC will be challenged to complete reviews in a timely manner with existing staff resources.

The OIPC has, in the past, had significant success in streamlining PIA review processes under the HIA. In particular, the Physician Office System Program (POSP), a joint initiative between Alberta Health, Alberta Health Services, and the Alberta Medical Association, was a major contributor to this efficiency. For seven

years, POSP provided PIA-writing, training and other support to physicians adopting electronic medical records. The OIPC was able to rely on this work to establish expedited PIA review processes, allowing for the efficient review of over 1600 PIAs. As a result of the program ending in March 2014, however, the OIPC can no longer rely on the expedited POSP PIA review processes. The OIPC expects the quality of electronic medical record PIAs to degrade over time without POSP consulting advice. Lower quality PIA submissions will mean increased OIPC review time.

Changes to the OIPC's office structure were made in 2013-14 to assist the Office in responding to the challenges identified above. In particular, the new structure provides an opportunity for the OIPC to review its processes to improve consistency, enhance efficiencies, and ultimately increase timeliness.

Nonetheless, anticipated and potential amendments to both the HIA and the FOIP Act will likely put additional strain on the Office in this regard.

2. Ability to identify and address access and privacy issues proactively for effective oversight

As already described, current stakeholder initiatives are increasingly complex, sophisticated, cross-sectoral, highly technical, interconnected and, most importantly, not always transparent to the individuals whose information is collected, used and disclosed.

The OIPC's traditional, primarily reactive, oversight model (responding to individual complaints and requests for review) is not adequate to provide effective oversight for these initiatives, or to reassure Albertans that their privacy is respected and protected. Because these initiatives are not always transparent to the public, it is not realistic for the OIPC to rely on complaints or requests for review as an indicator of legislative compliance. In fact, complaints submitted to the OIPC generally do not reflect the access and privacy issues and initiatives that stakeholders are primarily engaged with.[2]

Given the above, as part of the OIPC's restructuring in 2013-14, the Office established a Compliance and Special Investigations unit to specifically focus on proactive compliance, including PIA reviews and compliance investigations of systemic issues. Establishing this unit was a priority in 2013-14 and enhancing/building the program will continue over the next few years.

The need to proactively identify and address privacy and access issues has also been reflected in the OIPC's recent education and outreach efforts. Beginning in 2013-14, and continuing into 2014-15, the Office has focused resources on providing training workshops and seminars, rather than larger legislation-specific conferences. The first workshops focused on PIA training, breach response, and time extension requests with the intention of improving the quality of submissions to the OIPC over time. Demand for this training is expected to increase as the POSP program has been phased out and given anticipated and potential amendments to the HIA and the FOIP Act.

The OIPC has also allocated resources towards the Commissioner's mandate to engage in or commission research in order to get ahead of the issues and challenges facing stakeholders, and to contribute to increased awareness, understanding and

[2] OIPC Stakeholder Survey 2012

improved compliance. The results of two research studies will be made available in late 2014, focusing specifically on information sharing and the increased trend towards "deputizing the private sector".

Given the success of these initiatives to date, the OIPC will continue to look for opportunities to provide meaningful education, advice, research and training in advance, or in the absence, of receiving complaints.

3. Adequate staff and resources

OIPC resources are primarily invested in staff, and budget increases generally reflect in-range movement and cost of living. The number of OIPC staff increased by two positions in fiscal year 2012-13, and again by two positions in 2013-14, for a total of 42 full-time equivalents (FTEs).

As previously mentioned, over the last two years, the OIPC saw an overall 11 per cent increase in the total number of cases opened and a dramatic shift in the type of cases opened. The office restructure, implemented in 2013-14, reorganized the office teams based on function, instead of legislation. This restructuring was implemented to address the challenges from cases coming before the office, and to improve consistency and timeliness. As part of the restructure, the OIPC was able to reallocate one FTE position from corporate support services to an operational team to assist with caseloads.

In addition to the above, the OIPC will continue to work to manage limited resources as effectively and efficiently as possible by looking for opportunities to share support services with other Legislative Offices, collaborate with other access and privacy regulators to maximize resources and share expertise, and to ensure that OIPC information systems are enabled to support staff to perform as effectively and efficiently as possible.

4. OIPC staff members have the information, training and expertise required to provide effective oversight, guidance

The increasing proliferation of technology challenges the OIPC to stay on top of new developments. It is clear from the environmental trends and issues discussed earlier that technology underpins most of the significant initiatives that are underway in the public, private and health sectors. Ubiquitous technology (from biometrics to mobile devices, geo-location tracking software to the interoperability of information systems, social media to open data initiatives) is possibly the most significant factor affecting privacy and access to information today. In particular, the proliferation of electronic devices, the amount of data that can be stored on those devices, their increased portability, and the number of technology-related privacy breaches, give rise to concern.

It is imperative that OIPC staff be positioned to provide comprehensive and informed reviews of information systems and initiatives, and proactive guidance and direction to stakeholders who are grappling with new technologies. To address these issues, in 2013-14 the OIPC recruited a Senior Information, Privacy and Security Manager to enhance the Office's technological expertise.

In addition to keeping up with new technologies, OIPC staff also need to be aware of access and privacy issues that cross all sectors, as well as jurisdictions. Particularly with the advent of public/private/health partnerships, issues are no longer confined to any one sector. Even more importantly, there are opportunities for each sector to learn from the others. For example, the advanced technical work that is being completed in the health sector related to interoperable systems, self-serve health portals, and the

anonymization of health information for research purposes, has the potential to lead and guide in the public and private sectors. The mandatory PIA requirement under the HIA is another model that may have application outside of the health sector.

The OIPC's new office structure requires staff to have deep knowledge of all three Acts, and issues arising in each sector. Moving forward, the OIPC will focus on ensuring staff have opportunities to further develop expertise working with the three Acts. The OIPC will also actively work to develop technology expertise as well as broad knowledge and understanding of access and privacy issues.

5. Effective Knowledge Management

Many OIPC staff members have a long history with the Office. This means they have in-depth knowledge of the development and growth of the OIPC and the many issues that have been considered and resolved over the years.

Given the number, variety and increased complexity of issues before the Office, however, it is no longer feasible to rely on long-term staff members to be the source of all corporate knowledge. The OIPC is significantly disadvantaged each time a long-term staff member leaves the Office.

Further, the OIPC's case management system (TRAX) was initially built in 2001, and has only been incrementally tweaked over the years. The system was not designed to provide timely or meaningful access to information about the thousands of case files that have been resolved in the long history of the Office.

In 2012, the OIPC identified a need to more effectively manage corporate knowledge in order to improve the Office's capabilities and enable better decision-making. As a result, over the last two years, significant resources have gone towards a project to modernize the OIPC's case management system. Following the design, build and testing phases, the new system will be rolled out in early 2015. The new system is expected to significantly enhance the OIPC's ability to understand and report on the work of the Office, as well as to make decisions about process changes and allocation of resources

Another significant project that will be implemented in 2015 is a modernization of the OIPC website in order to improve communication with stakeholders and the public.

6. "Walking the talk"

The OIPC has a role to play in advocating for stakeholder adoption of access and privacy best practices, often beyond the legal requirements set out in the Acts.

Proactive disclosure of information is one such example. In December 2012 the OIPC expanded its own proactive disclosure to include the travel and hosting expenses of the Assistant Commissioner and OIPC Directors. In addition, the OIPC has started to report on the number and disposition of access requests made to it as a public body, as well as the number of privacy breaches experienced.

The OIPC continues to look for opportunities to proactively disclose information about its own operations as well as case work completed, including information about contracts and workload statistics, as well as PIA reviews and information about non-real risk of significant harm breach reports received. In addition, the OIPC plans to complete disaster preparedness activities, and initiate projects to test information systems security.

Goals and Key Strategies: 2015-2018

The following goals and strategies have been developed in acknowledgement of current environmental trends and issues, and to address the challenges described previously in the OIPC's Strategic Business Plan.

GOAL 1: Meaningful, proactive consultation and communication with stakeholders and the public

1.1 Identify and facilitate opportunities to consult with external stakeholders.
1.2 Publish guidance, direction and awareness materials to enhance stakeholder compliance.
1.3 Identify and facilitate opportunities to consult with other access and privacy regulators.
1.4 Plan, host and participate in workshops, conferences and educational forums to benefit stakeholders and the public.
1.5 Identify and facilitate opportunities to consult and engage with the public.
1.6 Publish proactive education, advice and direction for the public.

GOAL 2: Efficient, effective, timely processes

2.1 Consolidate and streamline intake, mediation and investigation processes to ensure they are fair, accessible, transparent, timely, high quality and consistent.
2.2 Review and revise adjudication processes as necessary to ensure they are fair, accessible, transparent, timely, high quality and consistent.
2.3 Build proactive compliance and special investigation function.
2.4 Build research and policy function within OIPC to support investigations, legislative review, proactive education, awareness and direction.
2.5 Establish and implement meaningful performance targets for OIPC staff.
2.6 Consider opportunities to share support services with other Legislative Offices.
2.7 Research models and consider merits of establishing Advisory function within the OIPC.

GOAL 3: Effective access to and use of OIPC information and resources

3.1 Enhance functionality of OIPC case management system (OB1).
3.2 Enhance functionality of OIPC website.
3.3 Establish accountable business planning and reporting processes.
3.4 Identify and facilitate further opportunities to proactively disclose OIPC information, datasets.
3.5 Review information management systems and schemes within OIPC to enhance efficiency and communication.
3.6 Review technology requirements to best support staff, efficient processes.
3.7 Enhance OIPC information security profile and research new technologies.

GOAL 4: Staff members are engaged, knowledgable and expert

4.1 Identify and facilitate opportunities for internal communication and consultation.

4.2 Identify and facilitate opportunities for internal team building.

4.3 Identify training requirements to ensure staff members are supported in their roles.

4.4 Ensure OIPC policies addressing key staff issues are in place and communicated to staff.

4.5 Ensure staff members have timely access to relevant local, provincial, national, and international news and information regarding access and privacy issues.